Staying anonymous, online & off.

October 1

2012

The need to knows about keeping your activities, aliases, and name secured from those whom it doesn't concern

An eBook by
AnonTech

Contents

Chapter 1: Staying secure locally (Offline) 2

Chapter 2: Staying secure online 4

Chapter 3: Miscellaneous & Wrap up 6

Chapter 4: Contact information, Credits, and Coming soon 7

Chapter 1: Staying secure locally (Offline)

So you want to stay anonymous offline and have a secure local network and computer? Well then you have come to the right place, in this chapter I will be showing you how to stay secure, programs to use, and what not to do to compromise your machine.

Part 1: Basics

Here are a few basic things to keep in mind when first starting to stay secure, and that's previous flaws. Please be mindful of what username on your computer that you are using, while unlikely it can connect a person to a computer. So using "Justin Blueballs" is probably not a good idea if that is your name. Another thing to be mindful of is the browser you are using. If you are using chrome, congratulations, you are part of a botnet. Uninstall that garbage and get a real browser, Firefox. I will discuss later what you should use to keep your browser secure.

Part 2: Programs

So you renamed your username and got your browser right? Well now you need to get some basic programs to secure your hard drive, information being transferred, written, and keystrokes.

Anti-Virus/Firewalls – So one of the first things you should get as a countermeasure is an Anti-Virus and Firewall. There are 2 things that come to mind that work great.

Malware Bytes Anti Malware – Find a way to get it, the registered version will come with a real time protection feature that comes in handy
Commando Firewall – A decent firewall that is not Microsoft's bloat ware they give you

So now that you have some suggestions, you are ready to move onto the next part. Realize that most AV/Firewalls will be sufficient and that is just my personal choices.

Encryption of keystrokes and data stored on Disk Drives – So now you have your computer secured from incoming threats as far as other hacktivists trying to compromise your machine, and information, let’s go to the next step, in case of you getting SWATTED or someone else tries to use third party software to read information off of your disks, we need to secure that. Here are the 2 necessities that come to mind to keep this information safe

Truecrypt – A nice piece of software to encrypt your data on your drives, using different algorithms and hash’s to secure your hard drive. It is freeware so you can pick it up on their website and use it as needed, it can even encrypt removable drives. When you encrypt, you will be asked to create an encryption key, make sure you use something no one will guess, and DO NOT write it down, keep it in your head. You will also be asked to create a recovery disk, if you do make it, put it in a remote location or break it on spot.

Key Scrambler – Now we move onto a key scrambler, you can pick them up for free if you know how, but basically what this program does is exactly what it is called. It scrambled your key strokes, for instance, you can be typing “Dog” and it will at random scramble with all valid keys, so it could come out “l1{“

Deep Freeze – This is a neat little program, It can also be attained for free if you know where to look. What this program does is when you have it in a “Frozen state” it basically takes a snapshot of your PC, with all its information and can roll back to that state at any time. This is great if you want to install something, have communications not logged on your PC, or a number of other things erased just by restarting.

Chapter 2: Staying secure online

Now that we have covered how to secure your machine locally, now it is time for the important part, staying secure online. This is by far the most important part to being secure, and not compromise who and where you are, and what you are doing.

Part 1: Basics

Here we go, you're ready to start doing what you want to do, but we have to make sure we have a few things checked off to make sure we are not going to fail prematurely.

- Do not, ever, log in to anything during your hacking session, this could lead to websites connecting your personal pages to them
- Do no use any personal information during your session, bad idea overall
- Absolutely DO NOT EVER accept any scripts or cookies while you are hacking or trying to be secure

Those are just some key points, just use common sense, and all should be good.

Part 2: Programs

Now we have to make sure are connection is secured, and no information is being logged, and if it is, that it has no trace back to us.

Changing your MAC address – So this is a pretty basic rule, considering each mac address can be linked back to a specific manufacture, and if you bought it at a store and used a rewards type card, it can even be traced back to you. So we want to change this

TMAC – So I don't know much about this program, all I know is it does change your MAC address; I on the other hand just do it manually.

Securing your network connection – We’re almost there, but now we have to make sure our connection to the internet is secure, The most secure way is a VPN (Virtual private network). I personally use iPredator as my VPN, it’s about $22 for 3 months, so it is reasonably priced.

TOR – Is a decent alternative to using a VPN, but you can be compromised more easily, if your exit node is doing traffic analysis, then he can read all traffic coming out. I would use this If you absolutely cannot afford a VPN.

Chapter 3: Miscellaneous & Wrap up

Woo! We did it. We went through most of the basics and covered some of the advanced. Now you're ready to take on the world, just remember to use common sense. I will cover a few other things that you might want to use, and end us with the conclusion of what we have learned in this eBook.

Part 1: Browser configuration

So, as a little side note, these plugins will be pretty damn helpful to keep us secure.

Blocking ads, scripts, and using SSL

Adblock Plus – By far my favorite plugin for Firefox of all time. This plugin will block 99% of all ads on the internet, so it creates a less annoying surfing experience, down to blocking ads on YouTube.

HTTPS Everywhere – So this plugin forces every website to use SSL if available, thus creating a more secure session, I would deem this a necessity.

No Script – This plugin blocks Java, Javascript, and Flash. This is where most of your information gets mined; sometimes you have to enable it on certain sites to get past security checks.

Part 2: Wrap up & summary

So let's review the concepts we have learned today. This should a nice double as a checklist.

1. Never use personal information while trying to stay secure
2. Secure your local connection before connecting to the internet, under no costs should you risk this
3. Make your online connection is secure as possible, and if you can't afford to do this, make use of what you have.

Chapter 4: Contact information, Credits, and Coming soon

So this is the end of my book, and I hope some of you have learned something from this, if so, then the effort to write it was worth it. As I am not very well known around HF, I wish to create a good name for myself. Finding multiple sources on the internet and mashing it up into an eBook is something I'm pretty good at. So I will be taking requests and having further releases on different subjects (XSS, SQLi, RATs, & More)

I would like to give credit to **Techie** for allowing me to you exerts of his mini tutorial on the same subject.

Contact information –

E-Mail: AnonTech@lavabit.com

Skype: Anontech

HF: AnonTech

Written By:

Anontech